AO-106 (Rev: 06/09)-Application for Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
Information Associated with the Google Account mikemartin4414@gmail.com that is Stored at a Premises Controlled by Google LLC

Case No. 24-mj-386-CDL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).
located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2261A	**Cyberstalking**
18 U.S.C. § 1512	**Witness Tampering**
18 U.S.C. §§ 1151, 1152 and 2242(3)	**Sexual Abuse without Consent in Indian Country**

The application is based on these facts:

See Affidavit of SA Audra Rees, attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Audra Rees, FBI
Printed name and title

Subscribed and sworn to by phone.

Date: May 24, 2024

Judge's signature

City and state: Tulsa, Oklahoma

Christine D. Little, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of Information Associated with the Google Account *mikemartin4414@gmail.com* that is Stored at a Premises Controlled by Google LLC	**Case No. _____**

Affidavit in Support of an Application for a Search Warrant

I, Audra Rees, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at a premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I have been employed as a Special Agent with the Federal Bureau of Investigation since January of 2020. I am currently assigned to work Indian Country Investigations for the Oklahoma City Division, Tulsa RA. As part of my duties as a Special Agent, I investigate criminal violations relating to crime in Indian Country, to include Sexual Abuse without Consent in Indian Country, Cyberstalking, and Witness Tampering.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2261A (Cyberstalking), and 18 U.S.C. § 1512 (Witness Tampering), and 18 U.S.C. §§ 1151,

1152 and 2242(3) (Sexual Abuse without Consent in Indian Country) have been committed by Michael Vincent Martin. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as further described in Attachment B.

Jurisdiction

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

6. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the government may obtain an order precluding Google from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Probable Cause

7. On March 18, 2024, B.R. reported that her ex-boyfriend, Michael Vincent MARTIN, had raped her the night before, March 17, 2024. B.R. said that MARTIN showed up at her house the night before, located at 2020 South 14th Street, Broken

Arrow, Oklahoma, which is within the Cherokee Nation in the Northern District of Oklahoma. MARTIN was drunk when he arrived and continued to drink at her house. B.R. decided to go to bed because MARTIN was being "hateful" towards her. Based on previous altercations with him, B.R. turned on her phone to record any interactions with MARTIN. Shortly after she went to the bedroom, MARTIN came into her room, took off his pants, and got into bed with her. MARTIN can be heard on the recording saying, "Should I drive home on Saint Patrick's Day, or should I have sex with the sleeping girl?" B.R. says "no." MARTIN began touching her and performing oral sex on her and says, "You shush, and I'll do this." He then says, "I know you want it, you can't say no." B.R. says, "no" again. B.R. tried to push MARTIN away with her feet but was afraid to resist too much because he has gotten violent with her in the past. MARTIN then began having sex with B.R. She told MARTIN to stop two or three more times and was crying. B.R. finally yells at MARTIN to "fucking stop" while she's crying. MARTIN says, "if you want me to stop, I will stop." Martin continued to have sex with B.R. for approximately 10 more seconds before stopping. As he is leaving, MARTIN says, "are you going to accuse me of something now?" B.R. tells MARTIN to just leave. MARTIN says he is sorry and leaves the house.

8. B.R. underwent a Sexual Assault Nurse Examination (SANE) on March 18, 2024.

9. On or about April 22, 2024, investigators accessed a link to a Google Drive provided by B.R. The Google Drive contained several different pieces of information. One of those was a folder titled "Emails after 03-17-2024".

10. This folder contained 95 screenshots of emails between MARTIN and B.R. MARTIN's google email address is mikemartin4414@gmail.com.

11. On March 18, 2024, MARTIN sent B.R. an email. In the email, he wrote: "What is going on? Why are you threatening me? The wedding you're in. What's going on?" B.R. replied with "You are not being threatened. Do not contact me again." MARTIN continued sending emails, and, near the bottom of the email said, "see you tomorrow night."

12. On March 19, 2024, MARTIN emailed B.R. many times. MARTIN told B.R. that he had "pushed the red button" and that he had to "strike back." MARTIN told B.R. he filed a protective order against her and a DHS case. Later, MARTIN told B.R., "I almost regret what I did today. Nah. You're evil. You'll see a field petition tomorrow and I hope you're back in time to be served. It'll probably happen Thursday actually so never mind." B.R. responded, "you filed a PO on me for what? And then why are you contacting me?" MARTIN told B.R. it was way worse than just a protective order, and that "the box has been opened" and she "asked for it." MARTIN then said, "I'll take it back I'm sorry ☹ I'm sorry. I'll take it back. I'll call DHS I'll try." B.R. told MARTIN she would appreciate it, and then MARTIN calls

her a "dumbass" and tells her that the protective order is just a precursor, and that he's reporting her for child abuse, child neglect and various other charges.

13. On March 19, 2024, MARTIN emailed B.R. and told her there is no "red button babe. I don't know what threats you thought I was making about getting you in trouble for something that doesn't exist something I can't name." MARTIN continues on before saying, "Before you go calling the police, I will not contact you again for the record. If you think, I don't accept responsibility for things on my own, try having a conversation about it."

14. On March 20, 2024, MARTIN emailed B.R. and told her that he was just trying to spook her, nothing he said is true, he didn't talk to anyone and hasn't done anything. MARTIN told her that he's sorry he made those "fake threats of getting you in trouble. They've all been fake."

15. Later on, March 20, 2024, MARTIN told B.R. "you ever claimed that I did anything that's a crime around you again believe me I will push the red button...."

16. MARTIN emailed B.R. on or about March 24, 2024, "Nah man. You're ficked up. You think my messaging you 100 times means I want you back."

17. MARTIN emailed B.R. on or about March 24, 2024, "you'll pay for your false accusations you made in that post," and "god i dont want to do it," and "try me bitch." MARTIN tells B.R. to stop "claiming victim hood."

18. In total, MARTIN emailed B.R. more than 300 times over the course of a week. These emails caused and were reasonably expected to cause substantial emotional distress to B.R.

19. On March 24, 2024, MARTIN called B.R. and she recorded the phone call. On the call, MARTIN is intoxicated and alternates between sobbing and yelling, and many parts are unintelligible. MARTIN says he's not an evil person, and maybe the alcohol made him a different person. He tells B.R. repeatedly that he loves her. MARTIN tells her that he doesn't know why she's angry. MARTIN said that B.R. lured him in so she could "claim rape" when it was "gray area" and she's not going to give him a chance to explain. B.R. told MARTIN that she told him "no" several times. MARTIN said that if that's how she felt then he's really sorry. MARTIN said he just didn't want to be accused of rape if she's recording it. B.R. asked MARTIN if he felt guilty for what he did. MARTIN says "yes, yes, yes." While sobbing, MARTIN says something about "punish fucking" B.R. because she slept with someone else. MARTIN then starts yelling at B.R. and told her that she made it a "gray area" on purpose so she could claim rape. MARTIN continues yelling and B.R. hung up the phone.

20. The FBI began investigating this case on April 5, 2024. On May 1, 2024, I made an appointment to meet with B.R. on May 6, 2024.

21. On May 4, 2024, B.R. and MARTIN were at Sheraton hotel, in Oklahoma City. B.R. tried to leave the hotel room because MARTIN was drunk and became

"mean." B.R. tried to leave two times, and both times MARTIN grabbed B.R., slammed her onto the bed, and restrained her. MARTIN told B.R. if she does not help get him out of his criminal charges, he will kill himself and it will ruin his family.

22. On May 5, 2024, B.R. and MARTIN were at her house in Broken Arrow. MARTIN knew about B.R.'s meeting with federal agents scheduled for May 6, 2024, and told her to lie about what happened and told her what to say. MARTIN had B.R. rehearse her statements repeatedly to practice.

23. On May 6, 2024, I met with B.R., her attorney Pamela Rains, and AUSA Stacey Todd at the U.S. Attorney's Office. B.R. attempted to recant the rape allegations and said that even though she "knew how the recording sounded," it was a consensual encounter.

24. On May 9, 2024, B.R. sent MARTIN an email and asked him not to contact her and told him she was going to file a protective order. B.R. went to the Tulsa County Courthouse to file a protective order against MARTIN. The Tulsa County Courthouse is located at 500 S. Denver Avenue, Tulsa, Oklahoma, which is located within the Muscogee (Creek) Nation Reservation in the Northern District of Oklahoma. As B.R. was leaving the courthouse, MARTIN walked up behind her and was crying and yelling at her and told her she was going to ruin his life. MARTIN followed B.R. back to her car and got into her car. B.R. told him to get out of the vehicle and eventually he got out. As she tried to leave, MARTIN blocked the

car and prevented her from leaving. B.R. rolled down her window and told him to move out of the way. MARTIN then tried to climb into her car through the window. B.R. began screaming and MARTIN left the area.

25. On May 9, 2024, at approximately 5 pm, an arrest warrant was issued for MARTIN in case 24-MJ-337-MTS. Tulsa Police and the FBI searched for MARTIN all evening, and he was able to evade arrest. At approximately 7:34 am on May 10, 2024, MARTIN texted a TPD officer and said he would surrender. MARTIN then called B.R. and said he just wanted to see her one last time. The FBI became very concerned that MARTIN might attempt violent action based on his previously suicidal statements and erratic behavior. TPD obtained an exigent ping on MARTIN's phone. TPD was able to locate him walking toward his truck outside of his apartment. TPD officers gave MARTIN commands to stop and MARTIN reached into his truck, giving officers severe safety concerns and concerns that he may have a firearm. After being ordered to stop again, MARTIN became compliant and was taken into custody. MARTIN asked the officers to leave his truck unlocked.

26. MARTIN had his briefcase on his person when he was arrested. Inside his briefcase, we located handwritten notes, with statements about what to tell B.R. to say to the FBI, what demeanor she should adopt during her meeting with the FBI, what questions the FBI was likely to ask, and that she should say the sex was consensual.

27. MARTIN's ex-girlfriend L.M. was also interviewed. L.M. and MARTIN dated from 2020 to 2021. L.M. said that MARTIN raped her on at least one occasion. L.M. said that despite blocking MARTIN and telling him not to contact her, he continued to contact her via phone and other applications. He sent her repeated text messages and voice messages. He also showed up to her home uninvited on multiple occasions. L.M. currently has an active domestic violence protective order against MARTIN, in Tulsa County case PO-2021-3387. MARTIN was present at and participated in a hearing on October 27, 2021, where the Court granted a final protective order for 5 years, and by its terms explicitly prohibited the use, attempted use, or threatened use of physical force against his former intimate partner and her child. L.M. has reported several violations of the protective order, after MARTIN contacted her via the phone.

28. Another ex-girlfriend of MARTIN's, V.J., reported that MARTIN raped her several times. They initially met in 2021 via a dating app. Their relationship ended in approximately October of 2021. Once their relationship ended, Martin sent V.J. repeated text messages, voicemails, and called her. When she blocked his phone number, he called from the *67 feature in order to connect the phone call. He also utilized other phone numbers. V.J. was unsure what apps or other methods he utilized to accomplish this. He also contacted her via social media. V.J. was so fearful of Martin she moved and changed her phone number so that he could not find her.

29. At all times relevant, B.R. was a member of the Cherokee Nation by blood and enrollment, roll number 260171. MARTIN is not Indian, as confirmed by B.R. and the five major tribes of Oklahoma, Cherokee, Muscogee (Creek) Nation, Choctaw, Seminole and Chickasaw.

Background Concerning Google[1]

30. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

31. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

32. Signing up for a Google Account automatically generates an email address at the domain "gmail.com." That email address will be the log-in username for access to the Google Account.

33. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

34. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if

a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

35. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

36. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

37. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

38. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

39. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

40. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date

and time) may be evidence of who used or controlled the account at a relevant time and can aid in locating the targets of an investigation. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

41. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

42. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators or other social media platforms. Social media platforms such as YouTube are often linked to other accounts or phone numbers utilized in furtherance of criminal activity. In addition, emails, instant messages, Internet activity, documents, and contact and calendar

information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

43. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

44. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar, so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

45. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

46. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with

me." Google preserves files stored in Google Drive indefinitely unless the user deletes them. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to back up all the data from their device to Google Drive.

47. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

48. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google

Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

49. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user

deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

50. A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-and-mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

51. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called "My Activity."

52. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to

Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts into automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

53. Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

54. Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward

phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

55. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users and location-based data.

Information to be Searched and Things to be Seized

56. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

57. Affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized

persons will review that information to locate the items described in Section II of Attachment B.

58. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, Affiant knows that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an

account that are relevant to an investigation but do not contain any searched keywords.

Conclusion

59. Based on the information above, there is probable cause to believe that there is evidence as described in Attachment B, of violations of Title 18, United States Code, Sections 1151, 1153, and 2242(3) (Sexual Abuse without Consent in Indian Country), Title 18, United States Code, Section 2261A (Cyberstalking), and Title 18, United States Code, Section 1512 (Witness Tampering) associated with the Google account described in Attachment A.

Respectfully submitted,

Audra Rees
Special Agent
FBI

Subscribed and sworn to by phone on May 24, 2024.

CHRISTINE D. LITTLE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with mikemartin4414@gmail.com ("the Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from January 1, 2020 to May 10, 2024, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

3. Telephone numbers, including SMS recovery and alternate sign-in numbers;

4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;

5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers;

6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs.

d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails.

e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

f. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

g. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded,

created stored, or shared with the account including drafts and deleted records; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

i. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

j. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

k. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;

l. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;

m. All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings and all associated logs, including access logs, IP addresses, location data, timestamps, and change history;

n. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

o. The types of service utilized;

p. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

q. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Sections 1151, 1153, and 2242(3) (Sexual Abuse without Consent in Indian Country), Title 18, United States Code, Section

2261A (Cyberstalking), and Title 18, United States Code, Section 1512 (Witness Tampering), including, for each account or identifier listed on Attachment A:

a. The contents of all communications, voicemails, txt messages, call logs, or other forms of communications between Martin and B.R., L.M., and V.J., or any other witnesses identified in this warrant;

b. Any communications, voicemails, text messages, call logs, or other forms of communications between Martin and any other party if the communication is deemed evidence by its connection to the described incidents, including individuals not yet identified.

c. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

d. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation, including notes, docs, sheets, and forms, lists and voice memos created by the account user;

e. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

f. The identity of the person(s) who communicated with the Account about matters relating to witness tampering and cyberstalking.

g. Internet and search browsing history and application usage, including search queries and clicks.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Certificate of Authenticity of Domestic Records Pursuant to Federal Rules of Evidence 902(11) and 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC ("Google"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. Such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature